APPLICATION FOR UNITED STATES PATENT

FOR

METHOD AND APPARATUS TO PROVIDE SECURED LINK

INVENTORS: GINZBURG, Boris;
FUDIM, Max;
KONDRATIEV, Vladimir.

INTEL REFERENCE NO.: P16744
EPLC REFERENCE NO: P-5907-US

Prepared by :Moshe Vegh

Intel Corporation.

94 Em-Hamoshavot Way
Ezorim Park, Building 2
Petach-Tikva 49527
Israel
Phone: (972) 3 9207513
Facsimile: (972) 3 9207509

METHOD AND APPARATUS TO PROVIDE SECURED LINK

BACKGROUND OF THE INVENTION

[0001] In wireless local area networks (WLAN), for example, WLANs that are based on IEEE-802.11-1999 standard, a basic service set (BSS) may include a set of stations, which may communicate with one another. In Some WLANs, for example, the BSS may include two stations (STA) and an access point (AP). In some of those WLANs, a first station (STA1) or a second station (STA2) may communicate with the AP but not with one another.

[0002] IEEE-802.11e-2003 draft, is an extension of the IEEE 802.11-1999 standard that introduced a mechanism for data packets transfer between two stations (e.g. STA1 and STA2) in the BSS. This mechanism may be referred and/or termed as "direct link" or "side traffic". However, the data packet that may be transferred according to the above described mechanism may not be transferred in a secured manner and the content of the data packets may be monitored by other stations of the WLAN.

BRIEF DESCRIPTION OF THE DRAWINGS

[0003] The subject matter regarded as the invention is particularly pointed out and distinctly claimed in the concluding portion of the specification. The invention, however, both as to organization and method of operation, together with objects, features and advantages thereof, may best be understood by reference to the following detailed description when read with the accompanied drawings in which:

[0004] FIG. 1 is a schematic illustration of a wireless communication system according to an exemplary embodiment of the present invention;

[0005] FIG. 2 is a block diagram of an access point according to an exemplary embodiment of the present invention;

[0006] FIG. 3 is a block diagram of a station according to an exemplary embodiment of the present invention; and

[0007] FIG. 4 is a flowchart of method to establish a secured communication link between at least two stations according to some exemplary embodiments of the present invention.

[0008] It will be appreciated that for simplicity and clarity of illustration, elements shown in the figures have not necessarily been drawn to scale. For example, the dimensions of some of the elements may be exaggerated relative to other elements for clarity. Further, where considered appropriate, reference numerals may be repeated among the figures to indicate corresponding or analogous elements.

DETAILED DESCRIPTION OF EMBODIMENTS OF THE INVENTION

[0009] In the following detailed description, numerous specific details are set forth in order to provide a thorough understanding of the invention. However it will be understood by those of ordinary skill in the art that the present invention may be practiced without these specific details. In other instances, well-known methods, procedures, components and circuits have not been described in detail so as not to obscure the present invention.

[0010] Some portions of the detailed description, which follow, are presented in terms of algorithms and symbolic representations of operations on data bits or binary digital signals within a computer memory. These algorithmic descriptions and representations may be the techniques used by those skilled in the data processing arts to convey the substance of their work to others skilled in the art.

[0011] Unless specifically stated otherwise, as apparent from the following discussions, it is appreciated that throughout the specification discussions utilizing terms such as, for example, "processing," "computing," "calculating," "determining," "establishing", "sending", "exchanging" or the like, refer to the action and/or processes of a computer or computing system, or similar electronic computing device, that manipulate and/or transform data represented as physical, such as electronic, quantities within the computing system's registers and/or memories into other data similarly represented as physical quantities within the computing system's memories, registers or other such information storage medium that may store instructions to perform actions and/or process, if desired.

[0012] It should be understood that the present invention may be used in a variety of applications. Although the present invention is not limited in this respect, the circuits and techniques disclosed herein may be used in many apparatuses such as stations of a radio system. Stations intended to be included within the scope of the present invention include, by way of example only, wireless local area network (WLAN) stations, two-way radio stations, digital system stations, analog system stations, cellular radiotelephone stations, and the like.

[0013] Types of WLAN stations intended to be within the scope of the present invention include, although are not limited to, mobile stations, access points, stations for receiving and transmitting spread spectrum signals such as, for example,

Frequency Hopping Spread Spectrum (FHSS), Direct Sequence Spread Spectrum (DSSS), Complementary Code Keying (CCK), Orthogonal Frequency-Division Multiplexing (OFDM) and the like.

[0014] Turning first to FIG. 1, a wireless communication system 100, for example, a WLAN communication system is shown. Although the scope of the present invention is not limited in this respect, the exemplary WLAN communication system 100 may be defined, for example, by the IEEE 802.11-1999 standard, as a basic service set (BSS). For example, BSS may include at least one communication station, for example, an access point (AP) 110, a station 120 (STA1) and a station 130 (STA2). In some embodiments, station 120 and station 130 may transmit and/or receive one or more data packets over wireless communication system 100. The packets may include data, control messages, network information, and the like. Additionally or alternatively, in other embodiments of the present invention, wireless communication system 100 may include two or more APs and two or more mobile stations. This arrangement of wireless communication system 100 may be referred by the IEEE 802.11 -1999 standard as an extended service set (ESS), although the scope of the present invention is not limited in this respect.

[0015] Although the scope of the present invention is not limited in this respect, in some embodiments of the present invention station 120 may communicate with AP 110 via a link 125 and station 130 may communicate with AP 110 via a link 135. In addition, stations 120 and 130 may communicate with one another via a link 140. Although the scope of the present invention is not limited in this respect, link 140 may be a direct link.

[0016] Although the scope of the preset invention is not limited in this respect, STA1 120 and STA2 130 may communicate over link 140 to transfer data packets, for example, according to the IEEE 802.11e standard, if desired. In addition, STA1 120 and STA2 130 may communicate over link 140 to transfer the data packets in a secured fashion, which will be described in detail below. In embodiments of the present invention, the transportation of the data packets over link 140 in the secure fashion may be performed according to a secure direct link protocol (SDLP), if desired.

[0017] Turning to FIG. 2, a block diagram of an access point (AP) 200 according to some exemplary embodiments of the present invention is shown. Although the scope of the present invention is not limited in this respect, AP 200 may include an antenna 210, a transmitter (TX) 220 to transmit radio frequency (RF) signals, a receiver (RX) 230 to receive RF signals, a SDLP controller 240, and a key generator 250 to provide pair-wise keys to STA1 120 and STA2 130, if desired.

[0018] Although the scope of the present invention is not limited in this respect, antenna 210 may be an omni-directional antenna, a monopole antenna, a dipole antenna, an end fed antenna, a circularly polarized antenna, a micro-strip antenna, a diversity antenna, and the like.

[0019] Although the scope of the present invention is not limited in this respect, antenna 210 may receive RF signals, which may include SDLP messages and/or data packets from STA1 120 and/or STA2 130. RX 230 may demodulate the RF signals to receive the data packets and/or to process the SDLP messages and may transfer the SDLP messages to SDLP controller 240. SDLP controller 240 may generate response messages and may provide the response messages to TX 220. TX 220 may transmit the SDLP response messages via antenna 210 to STA1 120 and/or to STA2 130, if desired. In some embodiments of the present invention, the pair-wise keys may be used to encrypt the data packets that are transferred over link 140, if desired. The pair-wise keys may be provided by key generator 250.

[0020] Although the scope of the present invention is not limited in this respect, key generator 250 may generate the pair-wise keys according to a selected encryption method, for example, robust security network (RSN) methods such as, for example, temporal key integrity protocol (TKIP), and/or cipher block chaining (CBC) counter mode (CCM) and/or Wi-Fi protected access (WPA) methods, and the like. In embodiments of the invention, key generator 250 may generate pair-wise keys that may be used with the selected encryption method, if desired.

[0021] Turning to FIG. 3, a block diagram of a station (STA) 300 according to some exemplary embodiments of the present invention is shown. Although the scope of the present invention is not limited in this respect, STA 300 may include at least one antenna 310 that may be used to transmit and/or receive data packets over wireless communication system 100 (FIG. 1), for example, WLAN. In embodiments of the

invention, antenna 310 may be an omni-directional antenna, a monopole antenna, a dipole antenna, an end fed antenna, a circularly polarized antenna, a micro-strip antenna, a diversity antenna and the like.

[0022] Although the scope of the present invention is not limited in this respect, STA 300 may include a transmitter (TX) 320, a receiver (RX) 330, a SDLP controller 340, a rate unit 350 that may store and provide at least one communication rate and/or a set of communication rates to SDLP controller, and a security module 360 to encrypt, decrypt and/or authenticate the data packets according to the selected security method. TX 320 and RX 330 may be used to transmit and/or receive packets over communication links, for example, link 140.

[0023] Although the scope of the present invention is not limited in this respect, SDLP controller 340 may receive information defining the communication rate from rate unit 350 and may receive information defining the security method from security module 360. In some embodiments of the present invention, SDLP controller 330 may provide and/or receive SDLP messages from an AP. For example, the SDLP message may include a request to establish a secured link, a response to the request or to requests, a "Success" message, an "Accept" message, or the like. Additionally or alternatively, the SDLP messages may include communication rate information, security method information, pair-wise keys, and the like. Although the scope of the present invention is not limited in this respect, SDLP controller 340 may include an application processor, a digital signal processor, a medium access controller, and the like. Additionally and/or alternatively, SDLP controller 340 may be implemented in software, in hardware and/or in combination of software and hardware.

[0024] Although the scope of the present invention is not limited in this respect, rate unit 350 may include a register and/or a memory, which may include the communication rate value and/or a plurality of other selectable communication rate values. In embodiments of the present invention, security module 360 may be implemented in software, in hardware, and/or in any suitable combination of software and hardware.

[0025] Turning to FIG. 4, a flowchart of method to establish a secured communication link between at least two stations according to some exemplary embodiments of the present invention is shown. Although the scope of the present

invention is not limited in this respect, the exemplary method may begin with STA1 (e.g. station 120 of FIG. 1) may send a SDLP request to an AP, for example, AP 110 (box 400), for example, to establish a secured direct link with STA2 (e.g. station 130 of FIG. 1). For example, the SDLP request may include a SDLP message that may include medium access control (MAC) addresses of STA1 and STA2, a supported communication rate set of STA1 and a supported encryption method and/or methods of STA1, if desired. Although the scope of the present invention is not limited in this respect, in the SDLP message, STA1 may be referred to and/or defined as an initiator of the SDLP, STA2 may be referred and/or defined as a recipient, and the AP may be referred and/or defined as a mediator.

[0026] Although the scope of the present invention is not limited in this respect, the AP may send the SDLP request to STA2 and, in return, STA2 may send a response to the AP (box 410). The response may include information on the ability of STA2 to support the SDLP. In some embodiments of the present invention, STA2 may not support SDLP. In those embodiments, the AP may send a "Reject" message to STA1 in order to terminate an attempt to establish the SDLP link. In some other embodiments of the present invention, STA2 may support SDLP. In those embodiments, the AP (e.g. AP 110) may send to STA1 and STA2 SDLP messages, which may include the supported communication rate set and the supported encryption method and/or methods, although the scope of the present invention is limited in this respect (box 420). The AP, for example AP 110, may select a communication rate from a subset of communication rates supported by both stations, and may select a common encryption method that may be supported by both stations.

[0027] Although the scope of the present invention is not limited in this respect, in some embodiments, wherein the RSN encryption method and/or methods may not be supported by both stations, e.g., STA1 and STA2 (box 430) or an wired equivalent privacy (WEP) encryption, e.g. IEEE 802.11 encryption protocol, is supported by both STA1 and STA2, then the AP may establish a secured link between STA1 and STA2 (box 470). After the establishment of the secured link, the stations (e.g. STA1, STA2) may exchange data packets in a secured fashion, if desired.

[0028] Although the scope of the present invention is not limited in this respect, if both stations may support similar RSN encryption method, for example CCM, TKIP,

or the like (box 430), then the AP may send a SDLP response to both stations. Such a response may include the subset of supported communication rates and the encryption method to be used between STA1 and STA2, for example, TKIP. In addition, the AP may exchange extensible authentication protocol (EAP) frames with STA1 and STA2 if desired.

[0029] In embodiments of the invention, an AP (e.g. AP 200 of FIG. 2) may generate pair-wise keys, for example, using key generator 250 (box 440) before the exchange of the EAP frames, if desired. In some embodiments, AP 200 may generate unicast TX and RX pair-wise keys that may be provided to STA1 and STA2. For example, STA1 may receive the MAC address of the STA2 and the unicast TX and RX pair-wise keys that may be generated according to the selected encryption method Furthermore, STA2 may receive the MAC address of the STA1 and the unicast TX and RX pair-wise keys that may be generated according to the selected encryption method. For example, AP 200 may send an "EAP accept" message that may include for example, the TX and RX pair-wise keys and the MAC address of STA2 or STA1, as desired (box 440). The stations (e.g. STA1 and STA2) may install the pair-wise keys and may respond to the AP with an "EAP success" message (box 460), if desired.

[0030] Although the scope of the present invention is not limited in this respect, the AP may establish the secured link by sending a "Ready" message to STA1 and STA2 (box 470). This may complete a handshake procedure between the AP and the stations. Subsequently, the stations (e.g. STA1, STA2) may exchange data packets in a secured fashion, if desired. When the data exchange is completed, the AP may send a "SDLP_End" message to STA1 and STA2 to end the SDLP session (box 480), if desired.

[0031] While certain features of the invention have been illustrated and described herein, many modifications, substitutions, changes, and equivalents will now occur to those skilled in the art. It is, therefore, to be understood that the appended claims are intended to cover all such modifications and changes as fall within the true spirit of the invention.